EL896636040US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Siani Lynne PEARSON, et al.)
Serial No.: Not yet assigned)
Filing Date: concurrently herewith) Our Ref.: B-4519 619565-9
For: "METHOD OF AND APPARATUS FOR INVESTIGATING TRANSACTIONS IN A DATA PROCESSING ENVIRONMENT") Date: February 22, 2002

CLAIM TO PRIORITY UNDER 35 U.S.C. 119

Commissioner of Patents and Trademarks
Box New Patent Application
Washington, D.C. 20231

Sir:

[X] Applicant hereby makes a right of priority claim under 35 U.S.C. 119 for the benefit of the filing date(s) of the following corresponding foreign application(s):

COUNTRY	FILING DATE	SERIAL NUMBER
GB	23 February 2001	0104580.6

[ ] A certified copy of each of the above-noted patent application was filed with the Parent Application No._____.

[X] To support applicant's claim, a certified copy of the above-identified foreign patent application is enclosed herewith.

[ ] The priority document will be forwarded to the Patent Office when required or prior to issuance.

Respectfully submitted,

Richard P. Berg
Attorney for Applicant
Reg. No. 28,145

LADAS & PARRY
5670 Wilshire Boulevard
Suite 2100
Los Angeles, CA 90036
Telephone: (323) 934-2300
Telefax: (323) 934-0202

THIS PAGE BLANK

GB9966360400

PATENTS • DESIGNS • COPYRIGHT • TRADE MARKS
The Patent Office

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

CERTIFIED COPY OF PRIORITY DOCUMENT

The undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1985 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

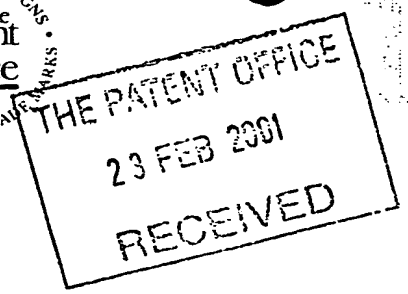
Signed

Dated 26 APR 2001

THIS PAGE BLANK (USPTO)

Patents Form 1/77

atents Act 1977
(Rule 16)



23 FEB 2001

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
South Wales
NP10 8QQ

1. Your reference — 30006595 GB

26FEB01 E608746-1 D01463
P01/7700 0.00-0104580.6

2. Patent application number
(The Patent Office will fill in this part) **0104580.6**

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

Hewlett-Packard Company
3000 Hanover Street
Palo Alto
CA 94304, USA

Patents ADP number *(if you know it)* 00149655800 1

If the applicant is a corporate body, give the country/state of its incorporation — Delaware, USA

4. Title of the invention — Method of and Apparatus for Investigating Transactions in a Data Processing Environment

5. Name of your agent *(if you have one)*

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

Richard A. Lawrence
Hewlett-Packard Ltd, IP Section
Filton Road
Stoke Gifford
Bristol BS34 8QZ

Patents ADP number *(if you know it)* 07563085001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

Yes

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	6
Claim(s)	2
Abstract	1
Drawing(s)	2 X 2

10. If you are also filing any of the following, state how many against each item.

Priority documents	-
Translations of priority documents	-
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	1
Request for preliminary examination and search *(Patents Form 9/77)*	1
Request for substantive examination *(Patents Form 10/77)*	-
Any other documents *(please specify)*	Fee Sheet

11. I/We request the grant of a patent on the basis of this application.

Signature Richard A. Lawrence Date 22/2/01

12. Name and daytime telephone number of person to contact in the United Kingdom

Meg Joyce Tel: 0117-312-9068

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500505.*

b) *Write your answers in capital letters using black ink or you may type them.*

c) *If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*

d) *If you have answered 'Yes' Patents Form 7/77 will need to be filed.*

e) *Once you have filled in the form you must remember to sign and date it.*

f) *For details of the fee and ways to pay please contact the Patent Office.*

METHOD OF AND APPARATUS FOR INVESTIGATING TRANSACTIONS IN A DATA PROCESSING ENVIRONMENT

Technical Field

The present invention relates to a method of and apparatus for investigating transactions, with an aim of identifying misdemeanour, in systems, institutions, or companies where such transactions are performed within a data processing environment.

Background Art

It has long been recognised that the power of computers can be utilised in order to commit fraud or other crimes. Some of these misdemeanours can be perpetrated by tampering with or subverting the processes run on a computer. The possibilities for committing such an act have been reduced by the advent of trusted computing platforms in which the integrity of the system is monitored through various stages of the system build commencing from power-up, loading of operating systems, and loading applications programs. However it is possible that users may take a more active role in committing fraud within a data processing environment, and in such circumstances it becomes desirable to launch an investigation.

Commencing an investigation is a highly sensitive task, especially when an investigation is being launched in one's own computing environment. Users must not be alerted to the fact that an investigation is in progress. However, this can be difficult to do since it will often be necessary to gain permission from system administrators in order to obtain the necessary access rights in order to perform the investigation properly. This can be counterproductive, especially when misdemeanour by administrators is suspected.

Disclosure of the Invention

According to a first aspect of the present invention, there is provided a method of investigating transactions in a data processing environment, which environment comprises a trusted computing environment, the method comprising the steps of:

(i) selecting a user within the trusted computing environment;

(ii) creating an investigation identity which is owned by the user;

(iii) using the investigation identity to take part in transactions; and

(iv) creating a record of those transactions.

It is thus possible to create an identity within the data environment solely for the purpose of performing the investigation. The record is trustworthy because it is created within a trusted computing environment.

In the present context, "trust" and "trusted" are used to mean that a device or service can be relied upon to work in an intended, described, or expected manner, and has not been tampered with or subverted in order to run malicious operations.

Advantageously the investigation identity is an anonymous identity. Within the context of electronic transactions, there has been growing concern over the amount of information swopped between two parties undertaking a transaction. Traditionally, in non e-commerce situations, a purchaser of a product or user of a service can go to the product or service provider and purchase that product or service anonymously if they transaction is a cash transaction. In order to overcome the perceived problem of not being able to remain anonymous, the concept of an anonymous identity has been proposed by the "trusted computing platform alliance" whose specification for a trusted computing platform can be found on their web site at www.trustedpc.org.

In essence, a user is given an electronic identity which contains no data concerning that user's physical identity. A trusted party maintains a record correlating the electronic identity with the user's physical identity. In a secure computing environment, a trusted platform is manufactured and then shipped/delivered with a manufacturer's endorsement that the device is a trusted platform. The owner of the platform chooses a privacy certification authority and enters a verification scheme, such as a TCPA protocol, involving a label chosen by the user, the trusted device in the trusted platform and the certification authority. During this process, the privacy certification authority binds the manufacturer's endorsement and the user's label into an identity certificate which is sent to the owner. This can be done a plurality of times with different certification authorities or with the same authority, thereby creating multiple identity certificates with different labels.

Consequently, parties to a transaction can be assured through the auspices of the trusted party that the entities that they are transacting with are authentic, whilst the entities can also remain anonymous.

Advantageously a user within a trusted computing environment is the owner of a plurality of identities. For example, the user could own one identity for carrying out work related tasks, could use and own a second identity for the purposes of conducting transactions such as buying records, books or the like, the user could use and own a third identity for carrying out a certain class of transactions which the user wished to keep segregated from other transactions, for example purchasing "adult material", and so on. In each case, each of the user's identities can be authenticated by a trusted party such that the user can undertake these transactions without his or her physical identity becoming disclosed. Of course, in the event of some misdemeanour, such as non-payment of bills, then the injured party can provide proof to the trusted party that this misdemeanour has occurred and then the trusted party can make the user's physical identity available such that the user can be pursued in order to remedy the misdemeanour.

The present invention builds upon the ability of a user to own an anonymous identity. For the purposes of the investigation, a new identity, namely an "investigation identity" is made which belongs to a selected user who has been selected by the originator of the request to perform an investigation, and by a service provider who performs the investigation, or who is the owner or operator of the trusted computing environment. Transactions using the investigation identity are preferably made by an investigator, who is not the user who owns the investigation identity.

Advantageously the user has the capability of monitoring transactions made using the investigation identity and also of suspending, removing, deleting or otherwise inhibiting the operation of the investigation identity. However, preferably, the user has no rights whatsoever to alter the record of transactions created using the investigation identity.

A description of event logging in a trusted environment can be found in the applicants co-pending International Patent Application Publication No. PCT/GB00/02004 entitled "Data Logging In Computer Platform", filed on 25 May 2000, the contents of which are incorporated by reference herein.

According to a second aspect of the present invention, there is provided an apparatus for investigating transactions, the apparatus including a trusted computing device arranged such that an investigation identity is owned by a user, and that a record of transactions made by the investigation identity is stored in an authenticated record by the trusted computing device.

Advantageously the record of transactions is authenticated and cannot be edited, except to add new transactions as and when they occur. Thus, the user and/or the investigating authority using the investigation identity only has the authority to create items within the record, but not to modify or delete any existing items.

The authenticity of the record can be trusted because the record is contained within a trusted computing device and the operation of that device can be trusted because it is authenticated by a trusted party.

According to a third aspect of the present invention, there is provided a computer program for causing a trusted computing device to perform the steps of the method according to the first aspect of the present invention.

Brief Description of the Drawings

The present invention will further be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 schematically illustrates a data processing arrangement including a trusted computing device which may be used for carrying out an investigation; and

Figure 2 schematically illustrates the steps performed in carrying out an investigation.

Best Mode for Carrying Out the Invention

As shown in Figure 1, a trusted computing device 2 has a memory 4, which can comprise a mass storage device such as a hard disc or tape, together with semiconductor memory such as RAM, which contains therein the information relating to a user 6 amongst other things such as an operating system, applications and data. The user may be the owner of multiple identities, labelled I_1, I_2 and I_3 in this example. The user's identity is, as noted herein before, maintained within a trusted computing device. In essence, a trusted computing

device includes a trusted module 10 which takes control of the computing device 2 at power-up or reset in order to ensure that the correct BIOS environment is built within the computing device. It can do this, either by containing the BIOS within the trusted device 10 or by possessing information about the correct nature of the BIOS such that the trusted device can validate the BIOS by examining check sums or the contents at specified addresses. Once the BIOS can be trusted, the operating system can then be installed over the trusted BIOS, and again the trusted device 10 can perform tests to validate the integrity of the operating system in order to ensure that neither the operating system nor the BIOS has been subverted. The trusted computing device 2 will typically also include input/output device 12, for example for driving video displays, receiving keyboard or mouse commands, and possibly removable storage media, as well as a communications device 14 which enables the trusted computing device to communicate with other devices in a data processing environment. A central processing unit 16 communicates with the memory 4, trusted device 10, input/output device 12 and communications device 14 via a data bus 18.

An exemplary trusted computing devise is further described in the applicant's co-pending International Patent Application Publication No. PCT/GB00/00528 entitled "Trusted Computing Platform", filed on 15 February 2000, the contents of which are incorporated by reference herein. Other forms of trusted computing devices can be envisaged by the skilled person.

The trusted computing device can communicate with other devices which may be local, or remote. Such links may be established over a distributed communications network 20, such as the internet. Other parties reachable and via the distributed communications network 20 may include a trusted party 22, and investigation agency 24 and a party 26 which party may be under investigation. In use, the investigation agency is given permission to use one of the identities, I_1 to I_3 as an investigation identity with which to undertake transactions with the party 26 under investigation. Thus, for example, identity I_3 may become a proxy identity for the investigation agency. Alternatively identity I_3 may have been specially created for this task. However, the investigation agency 24 is only given the rights to use the identity I_3, the ownership of that identity remains with the user whose identity 6 is maintained within the trusted machine 2. Thus, the user maintains

rights over the identity I_3, and in particular the right to suspend its use. This gives a level of control over the activities of the investigation agency 24 thereby allowing it to be brought to account and its activities to be constrained.

Figure 2 schematically illustrates a method of carrying out the present invention. The method commences at step 40 where it has been agreed, either by a law enforcement agency or an organisation, that an investigation should be commenced. An approach is then made to the investigation agency 24 in order to seek their assistance in the investigation. If the agency 24 agrees to participate, an individual is then selected at step 42 and their trusted machine 2 is used as a proxy for the investigations. The consent of the individual is required since the operation of their trusted machine cannot be subverted (because it is a trusted machine) and also because an anonymous identity owned by the individual is used by the investigation agency 24.

The selected user creates, at step 44, a new anonymous identity on their trusted computing machine 2 using the trusted computing platform application mechanisms that enable such anonymous identities to be created, and then allocates this new anonymous identity, I_3, to the investigation agency 24. The investigation agency can conduct transactions at step 46 using this identity, and a signed and authenticated log of all transactions is recorded at step 48. These logs are protected against deletion or alteration via the trusted component 10 on the trusted computing device 2. These logs can then be used as evidence in proceedings against any wrong doers. Periodically a check may be made at step 50 to see if the investigation has finished, if it has not further transactions may be conducted, otherwise the investigation is terminated at step 52 with the deletion of the investigation identity.

It should be noted that transactions are not merely restricted to entrapment operations where the investigation agency participates in the transaction. Thus, the investigation identity could also be used as a recipient of information as all information received by the investigation identity is authenticated and logged. Thus such an arrangement can be invoked for the collections of testimonies. Furthermore, the authenticity of the testator can be ascertained, even though that person's true identity remains known only to the trusted party 22 in accordance with the ability of a user to create an authenticated anonymous identity.

CLAIMS

1. A method of investigating transactions in a data processing environment comprising a trusted computing environment, the method comprising the steps of:

i. selecting a user within the trusted computing environment;

ii. creating an investigation identity which is owned by the user;

iii. using the investigation identity to take part in transactions; and

iv. creating a record of those transactions.

2. A method as claimed in claim 1, in which the investigation identity is an anonymous identity.

3. A method as claimed in claim 1 or claim 2, in which transactions made using the investigation identity are kept in an authenticated record by a trusted party.

4. A method as claimed in any one of the preceding claims, in which the record of transactions is made available to an investigator.

5. A method as claimed in any one of the preceding claims, in which the investigation identity is used by an investigator who takes part in the transactions.

6. A method as claimed in any one of the preceding claims, in which the user can monitor the transactions made using the investigation identity.

7. A method as claimed in any one of the preceding claims, in which the user can inhibit the operation of the investigation identity.

8. A method as claimed in any one of the preceding claims in which the trusted computing environment includes a trusted party who maintains the identities of parties to a transaction such that the identity of each party can be authenticated by other parties whilst each party is anonymous to the other parties.

9. An apparatus for investigating transactions, said apparatus including a trusted computing device arranged such that an investigation identity is owned by a user, and a record of transactions made by the investigation identity is stored in an authenticated record by the trusted computing device.

10. A computer program product for causing a trusted computing device to perform steps according to the method claimed in any one of claims 1 to 8.

ABSTRACT

METHOD OF AND APPARATUS FOR INVESTIGATING TRANSACTIONS IN A DATA PROCESSING ENVIRONMENT

(Figure 1)

A method of investigating misdemeanour within a data processing system is provided. An investigator is given an anonymous authenticated identity on a trusted computing device such that a trustworthy record of transactions can be created. The investigator can participate in the transaction.

Fig 1

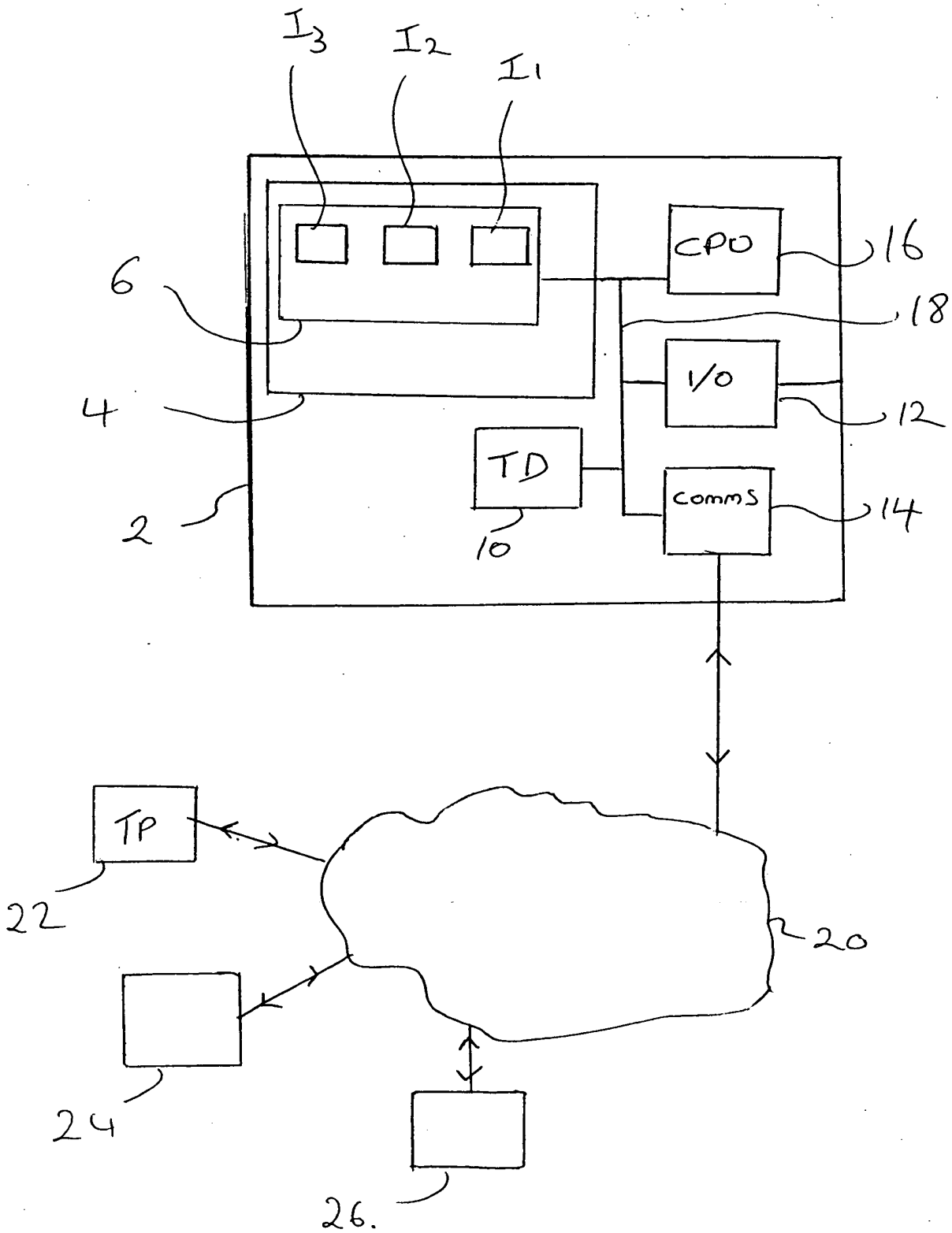
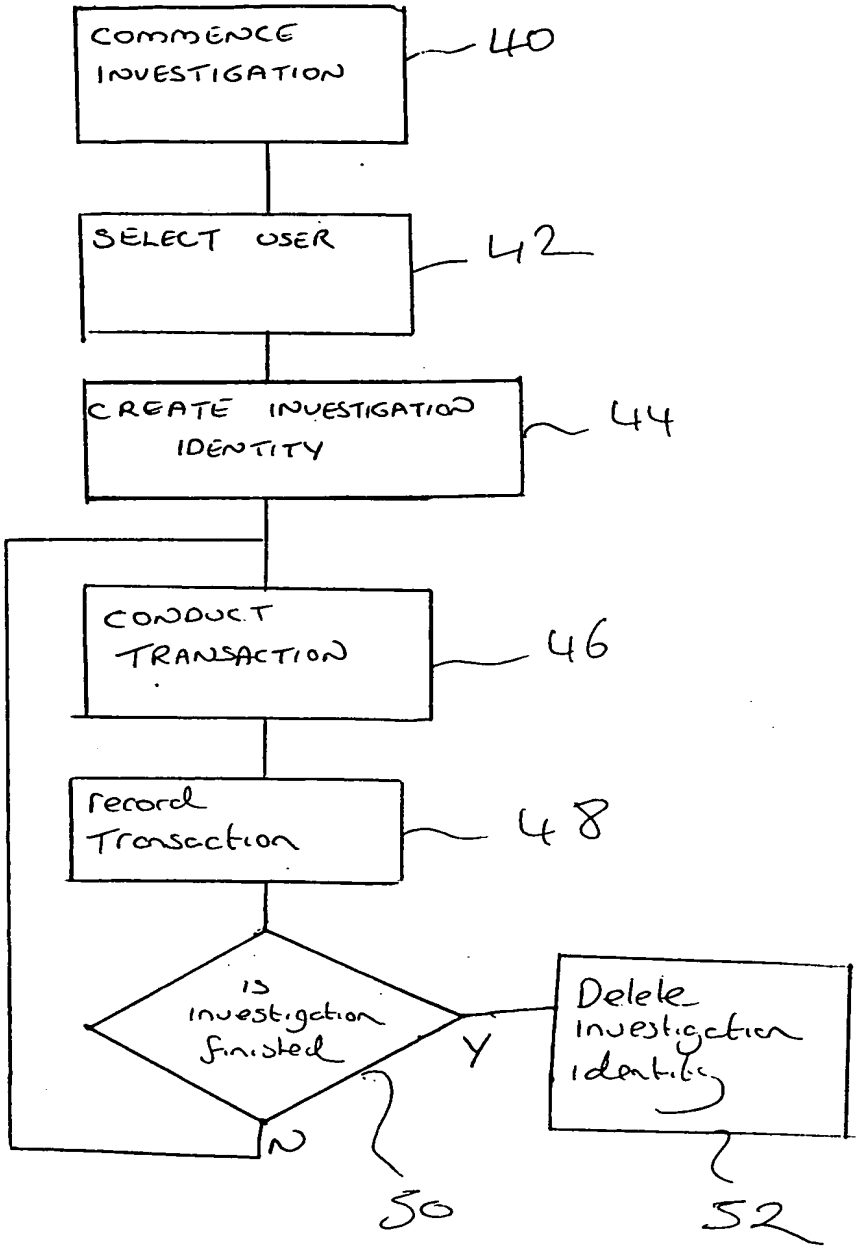


Fig 2


COMMENCE INVESTIGATION
40
SELECT USER
42
CREATE INVESTIGATION IDENTITY
44
CONDUCT TRANSACTION
46
Record Transaction
48
Is investigation finished
Y
N
Delete investigation identity
50
52